Navy fears computers make it prey to thieves

By Vernon A. Guidry, Jr.
Washington Bureau of The Sun

WASHINGTON – Top Navy supply officers don't believe any classified missile spare parts were lost to a recently disclosed West Coast theft ring working for Iran, but they worry that their aging computer systems have made the vast Navy supply system broadly vulnerable to insider thieves – whatever their motive.

These officers, who spoke on condition that they not be quoted by name, say the computer systems are not as vulnerable as they were when the system sailed on paper alone, but the current computerized operation is a product of the 1960s, when security for data processing systems was little developed, and not even much considered.

A huge modernization of Naval Supply Systems Command computer operations is under way, but it will be years before it is completed. "A big part of the upgrade of the system is to put absolute, state-of-the-art security into the software," said one officer involved.

"There is no question that a diverse, worldwide manual system can be ripped off in spades," said a high-ranking supply officer. "I suspect in days past we were being stolen blind. . . . In the computer age, we are at our most vulnerable point right now."

Speculation on the operation of the San Diego ring has centered on manipulation of the computer system. The current patchwork of different, aging and often incompatible computers used by the system "has been added, band-aided, manipulated and changed [to the point] that now nobody knows what is going on inside the system," said this officer.

"Now, when someone orders a coffee pot with the right number and we issue him a set of oars, we know something is wrong."

These officers do not believe that there is much of a problem with the so-called hacker, the outsider who intrudes into a computer system. It is the insider who is of concern. "The individual who has the right to use the computer, well, he probably has,

if he wants to go bad, the ability to manipulate it," says a knowledgeable officer.

The House Armed Services Committee is expected to have hearings on the security of the system and its computers in September.

The system has an inventory worth about $33 billion and manages some 16 million supply transactions a year. A spokeswoman for the system said no estimate on the loss to theft was available.

The supply system disperses spare parts and what are called "consumable items" through a series of regional supply centers and other Navy facilities such as air stations. Smaller installations, including shipboard supply facilities, draw from the larger centers. Items are ordered via computer codes and designations that identify not only the part but the requesting party as well.

The supply system has had its share of controversy in recent years. It was sharply criticized by Congress in the early 1980s for inventory lapses and has generated its share of spare parts "horror stories."

The most recent jolt came when seven persons were arrested, among them two Navy enlisted men and a civilian Navy warehouse employee, as part of an alleged ring that stole spare parts to Phoenix missiles and F-14 fighters to ship them to Iran. The United States had provided these weapons to Iran's former government but has banned spare parts sales to the current rulers of the country.

Since the San Diego arrests, Navy supply system officers have since checked the records of the classified portions of the missile system (there are 28 separate classified items) going to San Diego for the last two years and found no evidence that any of these parts was misdirected, at least as far as the supply system was concerned.

That conclusion was buttressed when federal prosecutors in San Diego said last week that the facts of the case would not support an espionage charge.

Speculation on the methods of the ring has centered on computer

manipulation. Items might be ordered using codes for, say, an aircraft carrier, directed to another location and intercepted somewhere in between, with the ordering facility and the receiving facility of record none the wiser, at least for a while. Few details on how the ring actually obtained a reported $5 million in stolen parts have been forthcoming from investigators.

Supply system officers here have been trying to piece the event together from their records, but they say they've been hampered by the tight compartmentalization that occurs when a federal criminal prosecution is undertaken. Top officers here say they get no details from the FBI until they're released publicly.

The Washington-based officers say they've uncovered no information yet that would definitely point to manipulation of the computer systems to steal the parts, but they're still looking. In the meantime, it is clear the parts had to be physically spirited from Navy facilities on the West Coast before they were shipped to Iran through intermediaries in New York and London.

The first phase of the computer modernization will be completed in 1987. It will cover planning and purchasing functions of the system at a cost of $349 million to $448 million, depending on future expansion. The second phase, to be completed much later, will cover the disbursing functions of the supply system, according to a spokeswoman.